(Rev. 01-31-2003)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 05/03/2007

To: Cyber **Attn:** CYBER US-CERT Liaison Rm 5965
SSA [redacted] b6
Attn: C3IU II Rm. 5931 b7C
SSA [redacted]

Tallinn **Attn:** Legat [redacted]

From: Dallas
Cyber
Contact: SA [redacted] b3 b6 b7C b7E

Approved By: [redacted]

Drafted By: [redacted]

Case ID #: [redacted]

Title: [redacted]

Synopsis: To open case and provide information to Cyber Division and Legat Tallinn.

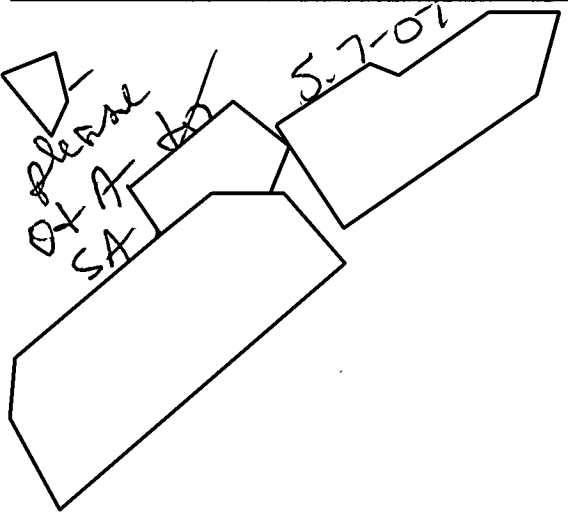
Administrative: 05/03/2007 telephone calls between SA [redacted] b6
Dallas Division and Cyber Division SSA's SSA [redacted] and SSA b7C
[redacted]

Details: At approximately 1630 EST on 05/02/2007, US-CERT was notified by the Department of Defense (DoD) Office of the Secretary of Defense that Estonia is currently under a national cyber attack. According to the source, the attacks consisted of DNS flooding root level servers. The origin of the botnet attacks are located in different geographic regions of the world; some coming from the United States (US). Estonia contacted the DoD as a North Atlantic Treaty Organization (NATO) member for assistance.

Recently, there has been unrest and rioting in the country of Estonia. CNN has reported that police have arrested approximately 600 people and 96 were injured during clashes in Estonia's capital over the removal of a disputed World War Two Red Army monument; Russia has reacted furiously to the moving of the monument. Estonia has said the monument had become a public order menace as a focus for Estonian and Russian nationalists.

[redacted] b6 b7C b7E

b3
b6
b7C
b7E



To: Cyber From: Dallas
Re: [redacted]

b3
b7E

LEAD(s):

Set Lead 1: (Info)

CYBER

AT WASHINGTON D.C.

For information only.

Set Lead 1: (Info)

TALLINN

AT TALLIN, ESTONIA.

For information only.

♦♦

To: Cyber From: Dallas
Re: [redacted] b3 b7E

On 05/03/2007, SA [redacted] contacted the United States Attorney's Office, Northern District of Texas to request 2703(d) non-content letters [redacted] b6 b7C b7E

Inasmuch as the attacks are targeting the infrastructure of an NATO member and computers within the Dallas Division are attacking the infrastructure, it is recommended a case be opened and assigned to SA [redacted] b6 b7C

To: Cyber From: Dallas
Re: [redacted] b3 b7E

Upon receipt of notification of the incident from DoD, US-CERT coordinated with the private sector and attained a list of the attacking IP addresses. Through more in-depth analysis US-CERT has the following information:

Currently 2,521 unique IP's have been identified as part of the attacking botnet(s), of which 290 are US-based. Of those 290, there are approximately 50 Internet Service Providers (ISP) listed. The majority of the attack appears to be originating from Russia. The following sites were identified as targets as of 29 April 2007:

www.peaminister.ee (Website of the prime minister)
www.reform.ee (Party of the prime minister)
www.agri.ee (Ministry of Agriculture)
www.kul.ee (Ministry of Culture)
www.mod.gov.ee (Ministry of Defence)
www.mkm.ee (Ministry of Economic Affairs and Communications)
www.fin.ee (Ministry of Finance)
www.sisemin.gov.ee (Ministry of Internal Affairs)
www.just.ee (Ministry of Justice)
www.sm.ee (Ministry of Social Affairs)
www.envir.ee (Ministry of the Environment)
www.vm.ee (Ministry of Foreign Affairs)
www.pol.ee (Estonian Police)
www.valitsus.ee (Estonian Government)
www.riigikogu.ee (Estonian Parliament)

Nine of the attacking IP address attacking the Estonian websites are located in the Dallas Division and are registered to SBC Internet Services.

[redacted] b6 b7C
- SBC Internet Services
- SBC Internet Services
- SBC Internet Services
- SBC Internet Services
- SBC Internet Services
- SBC Internet Services
- SBC Internet Services
- SBC Internet Services
- SBC Internet Services

In referenced telcals, SSA [redacted] and SSA [redacted] advised SA [redacted] further information regarding the Botnet was being gathered from US-CERT, Microsoft and the Argonne Ridge Group. FBIHQ will forward any copies of the involved Malware to Dallas Division. SSA [redacted] also forwarded a list of attacking IP addresses which will be kept in the 1A section of the file. b6 b7C

[redacted](DL) (FBI) b3 b6 b7C b7E

From: [redacted](DL) (FBI)
Sent: Wednesday, May 30, 2007 9:00 AM
To: [redacted](CyD) (FBI)
Cc: [redacted](DL) (FBI)
Subject: FW: Estonian Cyber Attacks [redacted]

UNCLASSIFIED
RECORD [redacted]

Sorry [redacted] I should have copied you in on this earlier todauy, I knew questions would come up.

[redacted] do you have anything to add to this?

[redacted]

-----Original Message-----
From: [redacted](DL) (FBI)
Sent: Wednesday, May 30, 2007 7:42 AM
To: [redacted](TL) (FBI)
Cc: [redacted](CyD) (FBI); [redacted](DL) (FBI)
Subject: RE: Estonian Cyber Attacks [redacted]

UNCLASSIFIED
RECORD [redacted]

We do not have results as of yet concerning the IP addresses we were provided. As soon as Dallas as information we will forward that to you.

Thanks,
SSA [redacted]
Dallas

-----Original Message-----
From: [redacted](TL) (FBI)
Sent: Wednesday, May 30, 2007 1:37 AM
To: [redacted](CyD) (FBI)
Cc: [redacted](CyD) (FBI); [redacted](TL) (FBI); [redacted](OIO) (FBI); [redacted](OIO) (FBI); [redacted](TL) (FBI); [redacted](DL) (FBI); [redacted](DL) (FBI)
Subject: Estonian Cyber Attacks [redacted]

UNCLASSIFIED
RECORD [redacted]

[redacted]

Below are two articles from yesterday here that have interesting information. We will continue to follow up with Estonian CCP and KAPO as the dust settles further.

Anything that can be done on the U.S. side to source these attacks (i.e. information from the Dallas case) would be very useful for us to pass.

NASHI is closely supported by the Russian government. BNS is the Baltic News Service and usually credible.

[redacted]

The newspaper said this was not true, and that just like in Russia a cyber offense like this was punishable with four to seven years in prison in the region.

Vedomosti added that no punishment was likely to follow since Estonia did not formally recognize Transnistria.

Goloskokov told Vedomosti he didn't know who else had staged cyber attacks on Estonia. He also said he didn't coordinate his actions with Nashi's leaders.

One of the best-known hackers in Russia, appearing under his web alias SpORaw, told the newspaper that the most efficient online attacks on Estonia could not have been carried out without the help of the Russian state. He said the hackers apparently acted under orders or instructions from parties in higher positions.

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

Assistant Legal Attaché
Estonia, Latvia, Lithuania
U.S. Embassy Tallinn

[redacted]

b6
b7C
b7E

TALLINN, May 29, BNS - Even though large-scale cyber attacks against Estonia ceased about two weeks ago, separate minor attacks against Estonian websites continue to take place, officials say.

The separate attacks against the Estonian cyberspace that can still be observed are unable to disrupt normal service, said Rica Semjonova, head of communications for the Estonian Informatics Center.

To fend off attacks against Estonia, IT security specialists at Estonia's state institutions and businesses continue to work closely with CERT organizations dealing with information security incidents from around the world.

Also the European Parliament has drawn attention to the cyber attacks, calling on the European Commission and all EU member states in a resolution adopted last week to take part in analyzing of the cyber attacks and look how to fight against such attacks in the EU. It also called on Russia to support the inquiry.

Major cyber attacks against Estonian websites began on April 27, a day after the beginning of street riots in Tallinn. Some of the cyber attacks against Estonia came from computers whose IP addresses referred to the Kremlin administration.

COMISSAR OF NASHI SAYS HE WAGED CYBERATTACK ON ESTONIAN GOVT SITES

TALLINN, May 29, BNS - Konstantin Goloskokov, a comissar of the pro-Kremlin Russian youth movement Nashi (Ours), has said that one of the cyberattacks against Estonia was staged by him together with a few friends.

Goloskokov told the Russian newspaper Vedomosti that he came upon the idea as he learned about the removal of the Bronze Soldier monument in Tallinn while in Transnistria, the separatist region of Moldova.

"Everybody thought that the statue would stand at least until May 9, its removal was a shock, and we decided to express our protest," Russia's Rosbalt news agency quoted Goloskokov as telling the newspaper. "We considered an attack on the web pages of the Estonian government as the most adequate response," he said.

Preparations took two days, and on the night before May 1 Goloskokov and three of his friends attacked the web sites of the Estonian Ministry of Defense, Ministry of Interior, the president, and the portal of Estonian government sites at www.riik.ee.

Infected computers situated in Hungary, Germany and South Korea were used to carry out the attack, he said.

The newspaper said Goloskokov was the only person to have admitted standing behind the cyber attacks on Estonia so far.

The young man is not afraid of punishment because such actions are not punishable in Transnistria, as he learned from local law enforcement bodies.

[redacted] (DL) (FBI) b3 b6 b7C b7E

From: [redacted] (DL) (FBI)
Sent: Wednesday, May 30, 2007 9:59 AM
To: [redacted] (DL) (FBI); [redacted] (TL) (FBI)
Cc: [redacted] (CyD) (FBI); [redacted] (CyD) (FBI)
Subject: RE: Estonian Cyber Attacks [redacted]

We have 2703 orders for the victim systems of Comcast/Cox Communications/Verizon/SBC/Road Runner (aka Time Warner) and Inktomi Corporation. Which were the ISPs with the most victims. The articles you provided are in line with all the other articles we have seen, indicating the controllers are in Russia. In addition to the 2703 orders for disclosure we have contacted Argonne Ridge Group and Microsoft. As soon as Dallas is provided information we will update.

SA [redacted]
FBI - Dallas Cyber Squad
tel
cel [redacted]

-----Original Message-----
From: [redacted] (DL) (FBI) b3 b6 b7C b7E
Sent: Wednesday, May 30, 2007 7:42 AM
To: [redacted] (TL) (FBI)
Cc: [redacted] (CyD) (FBI); [redacted] (DL) (FBI)
Subject: RE: Estonian Cyber Attacks [redacted]

UNCLASSIFIED
RECORD [redacted]

We do not have results as of yet concerning the IP addresses we were provided. As soon as Dallas as information we will forward that to you.

Thanks,
SSA [redacted]
Dallas

-----Original Message-----
From: [redacted] (TL) (FBI) b3 b6 b7C b7E
Sent: Wednesday, May 30, 2007 1:37 AM
To: [redacted] (CyD) (FBI)
Cc: [redacted] (CyD) (FBI); [redacted] (TL) (FBI); [redacted] (OIO) (FBI); [redacted] (OIO) (FBI); [redacted] (TL) (FBI); [redacted] (DL) (FBI); [redacted] (DL) (FBI)
Subject: Estonian Cyber Attacks [redacted]

UNCLASSIFIED
RECORD [redacted]

[redacted]

Below are two articles from yesterday here that have interesting information. We will continue to follow up with Estonian CCP and KAPO as the dust settles further.

Anything that can be done on the U.S. side to source these attacks (i.e. information from the Dallas case) would be very useful for us to pass.

NASHI is closely supported by the Russian government. BNS is the Baltic News Service and